eSecurity

Treinamentos em Segurança da Informação

O que temos para hoje?

Menu do dia:

- ✓ **Brute Force:**
  - ✓ Falhas de Engenharia Social
  - ✓ Wordlist personalizado
  - ✓ Wordlist utilizando redes sociais
  - ✓ Entendo Rainbow Tables
  - ✓ Trabalhando com Rainbow Tables
  - ✓ Entendendo o processo de Salt da Microsoft

Brute Force

Brute Force: Eng. Social

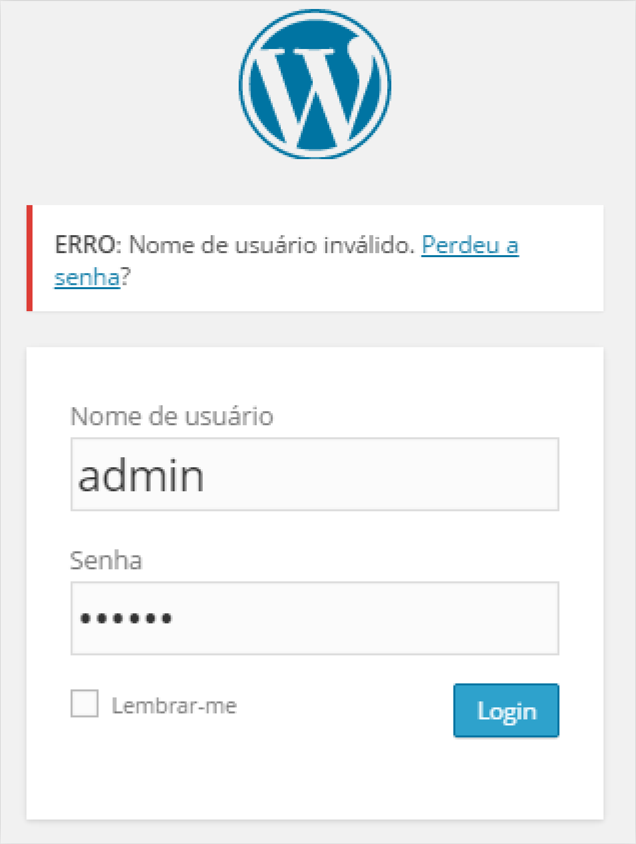
Existe uma falha, não muito explorada, que revela a existência ou não de um determinado usuário, ou seja, sabemos que um processo de brute force, saber o usuário e tentar descobrir a senha, economiza em 50% o ataque.

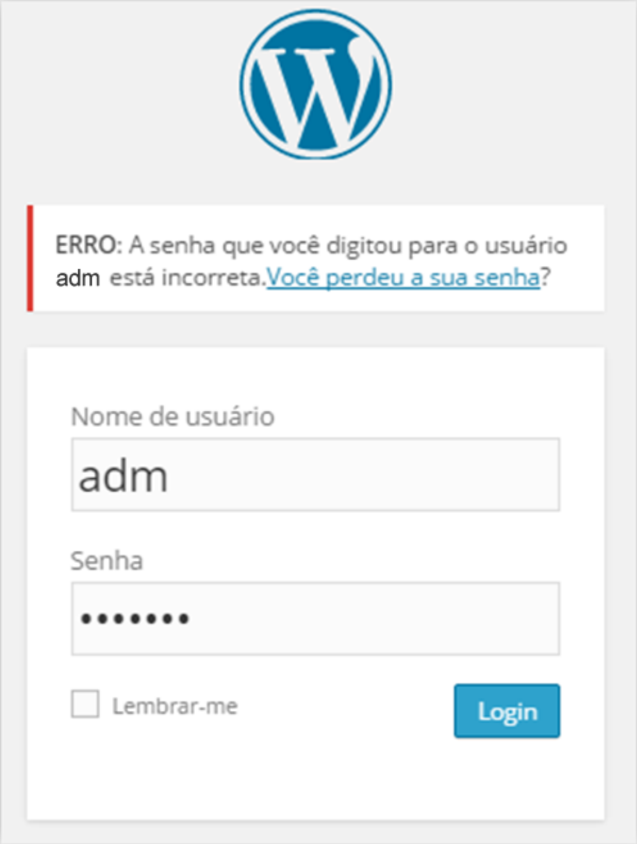
É considerado falha de segurança o sistema que informa que o usuário não existe e o outro que informa apenas que a senha está incorreta.

De modo que é importante sempre obter a tal da Segurança por Obscuridade e nunca revelar a existência de um usuário, mas sim a negativa do acesso ao sistema, ele existindo ou tendo apenas a senha incorreta.

Brute Force: Eng. Social

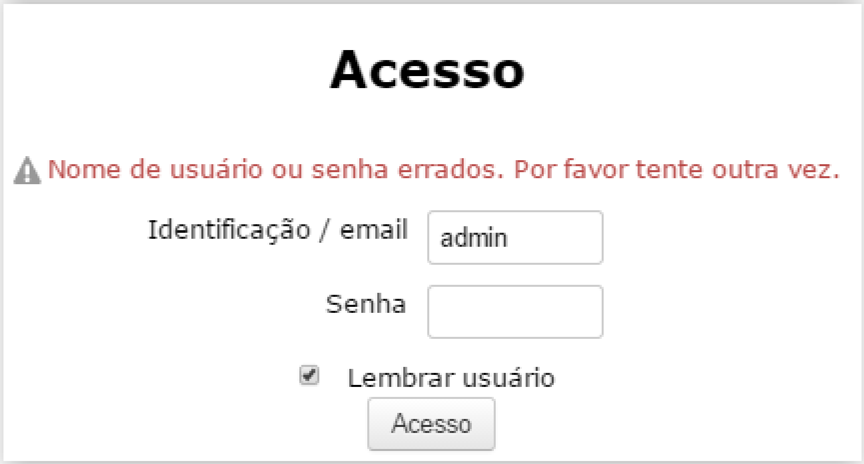
Método errado

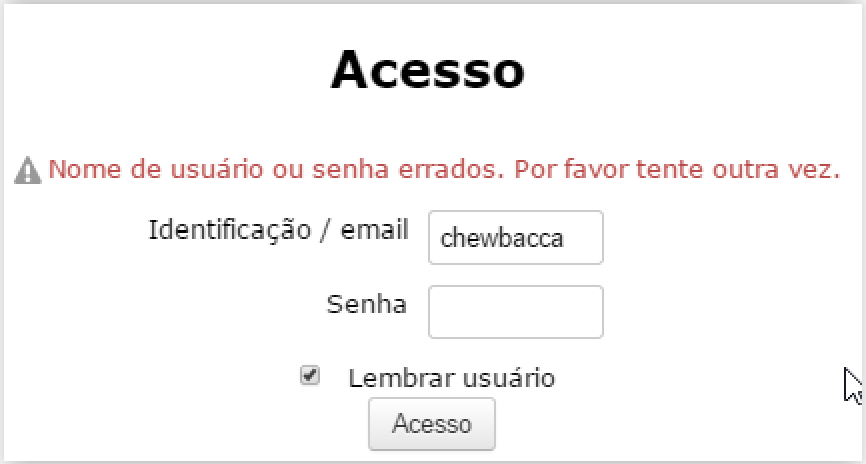




Brute Force: Eng. Social

Método correto





Perceba que as duas mensagens de erro são iguais para usuários que existem e para os que não existem

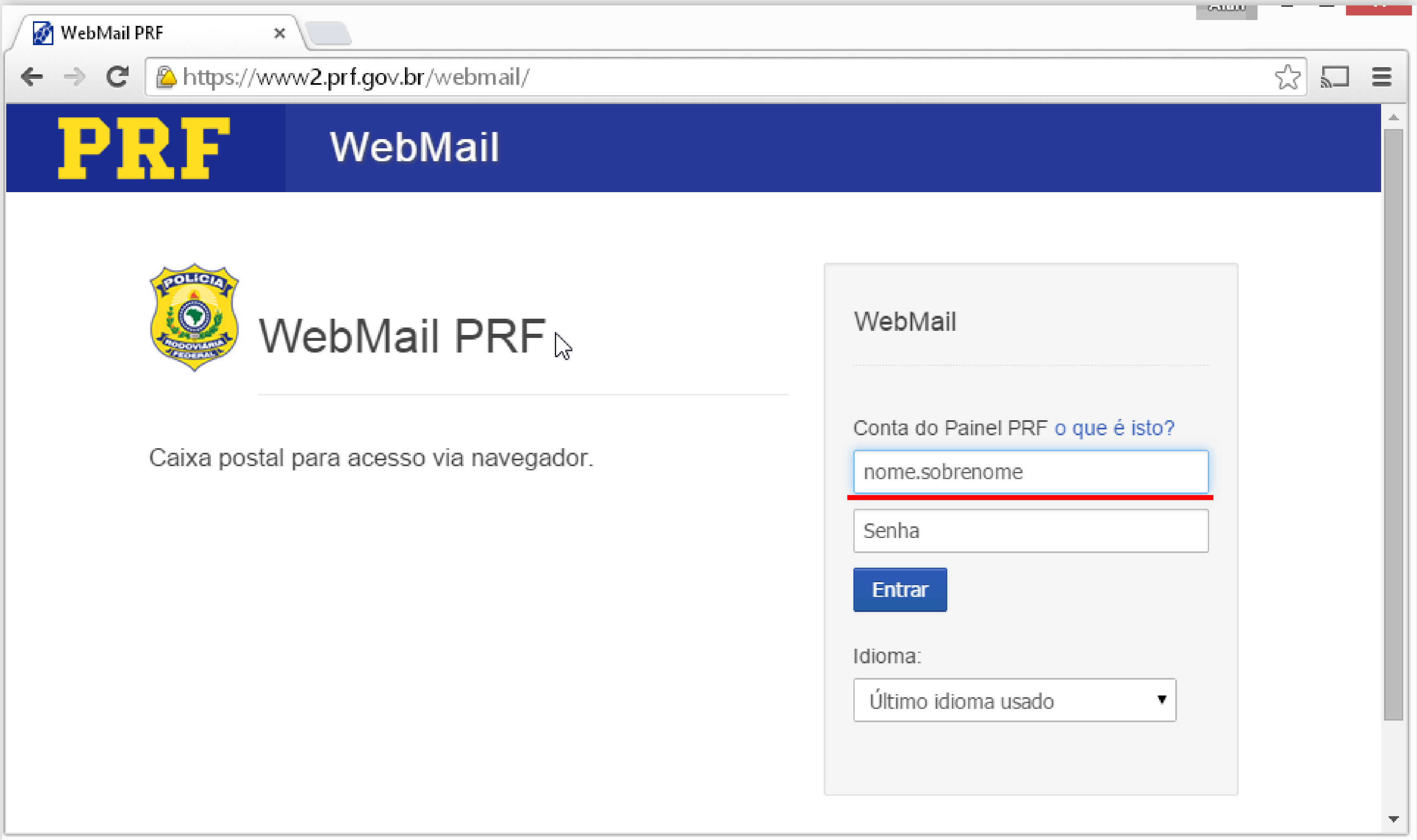
Brute Force: Eng. Social

A utilização da Engenharia Social é extremamente útil, porém, existem casos que, mesmo com o uso da engenharia social, pode-se utilizar técnicas para diminuir os riscos, tais como o uso do captcha.

O atacante consegue efetuar a descoberta do usuário, porém, não consegue realizar o ataque de brute force.

Facilitar esses métodos, é estar conivente com possíveis ataques, conforme apresentado abaixo:

Brute Force: Eng. Social



Brute Force: Eng. Social

Brute Force: Eng. Social

Não realizamos testes no ambiente, visto que, não temos autorização para isso.

Mas é possível ter uma pequena noção das falhas que podemos enfrentar em nosso cliente.

1. Veja que no site da PRF solicita o nome.sobrenome, deixando bem claro como é o sistema de autenticação utilizado, assim, facilitando e muito a vida de um atacante.

2. Não existe um captcha, sendo assim, podendo realizar um brute force.

3. É fácil encontrar o usuário através do google, bastaria apenas o atacante usar uma wordlist.

Brute Force: Personal Wlist

Ter uma super wordlist, com mais de 15gb de palavras e tentar utilizar contra todos os alvos que você encontrar, não é recomendado.

Vamos imaginar que você está auditando um site nos EUA, e encontrou um serviço de SSH, nele você tenta utilizar a sua wordlist, que contém milhares de palavras em português. Agora devemos nos perguntar...

Qual é a possibilidade da senha do serviço SSH nos EUA ser, sei lá, melancia?
Com certeza é muito menor.

Geralmente os americanos utilizam palavras de seu dicionário acompanhados de um número no final, por exemplo:
snowing1, moving9, world5.

No Brasil, os hábitos são diferentes, usa-se muito o 123 no final de algumas palavras, como por exemplo:
Teste123, teste@123, 123mudar...

Brute Force: Personal Wlist

Um técnica que funciona bem, é o ataque direcionado, ao qual é criado uma wordlist de acordo com o perfil do alvo.

Vamos seguir alguns passos:

1. Identifique seu cliente
2. Procure pelos responsáveis do serviço a ser atacado, geralmente analistas de infraestrutura, geralmente no Linkedin
3. Busque informações pessoais, geralmente no facebook
4. Monte sua wordlist de acordo com os dados coletados, ex: Time, filhas(os), mulher(marido), pets, etc..

Brute Force: Personal Wlist

LinkedIn

Ricardo Rossini Bonsangue

113 conexões

Analista de Suporte Técnico PL. da empresa Alstom Group

São Paulo e Região, Brasil | Tecnologia da informação e serviços

Atual	Alstom Brasil Energia e Transporte Ltda.
Anteriores	Alstom Transport, Alstom Brasil Energia e Transporte Ltda.
Formação acadêmica	FIAP

Cadastre-se no LinkedIn e acesse o perfil completo de Ricardo. É grátis!

Faça como 300 milhões de profissionais e cadastre-se no LinkedIn para compartilhar conexões, ideias e oportunidades.

- Visualize quem vocês conhecem em comum
- Solicite uma apresentação
- Entre em contato direto com Ricardo

Visualize o perfil completo de Ricardo

Experiência

Analista de Suporte Técnico PL.

Alstom Brasil Energia e Transporte Ltda.

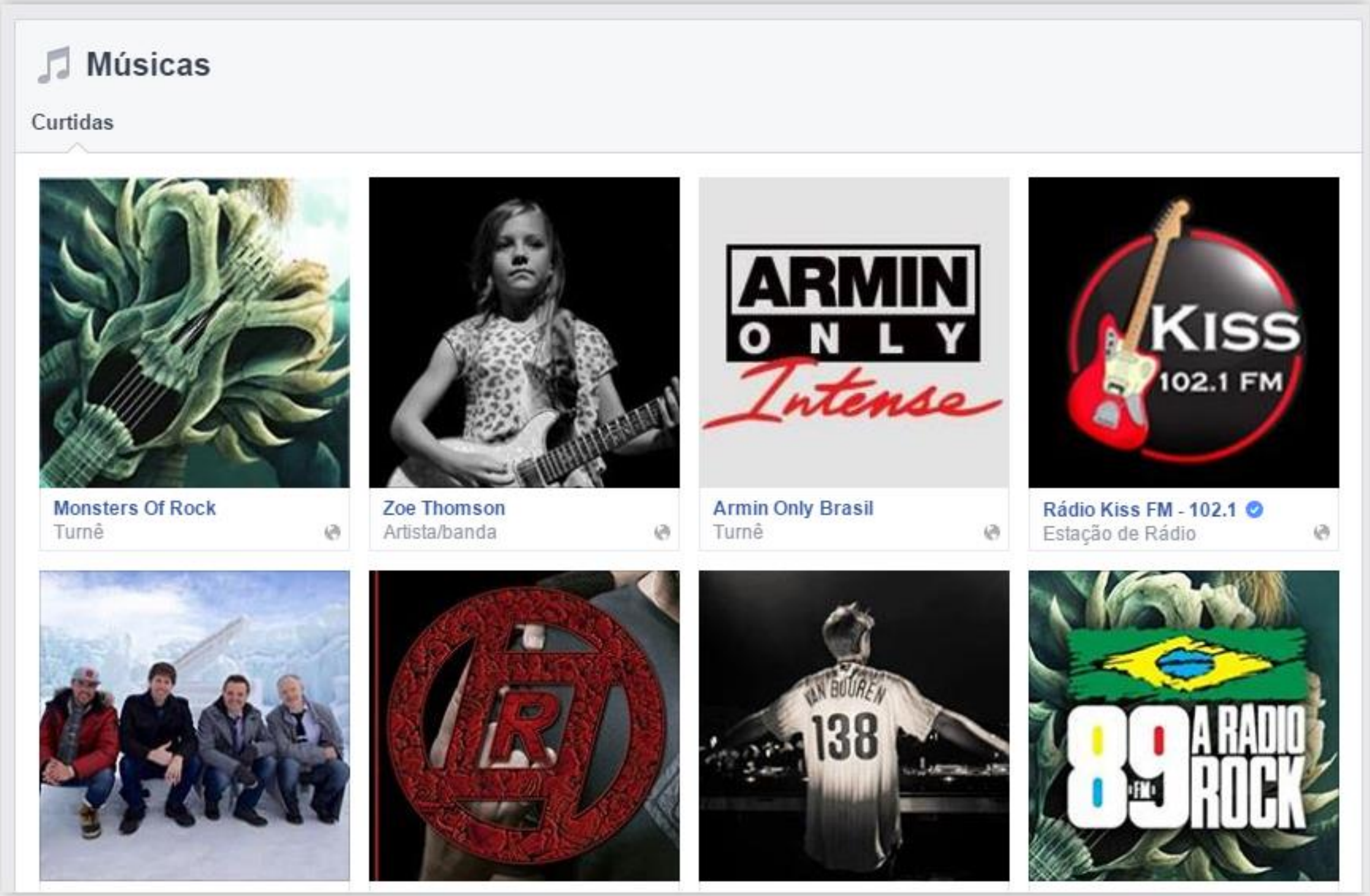
abril de 2013 – até o momento (1 ano 11 meses) | Lapa

ALSTOM

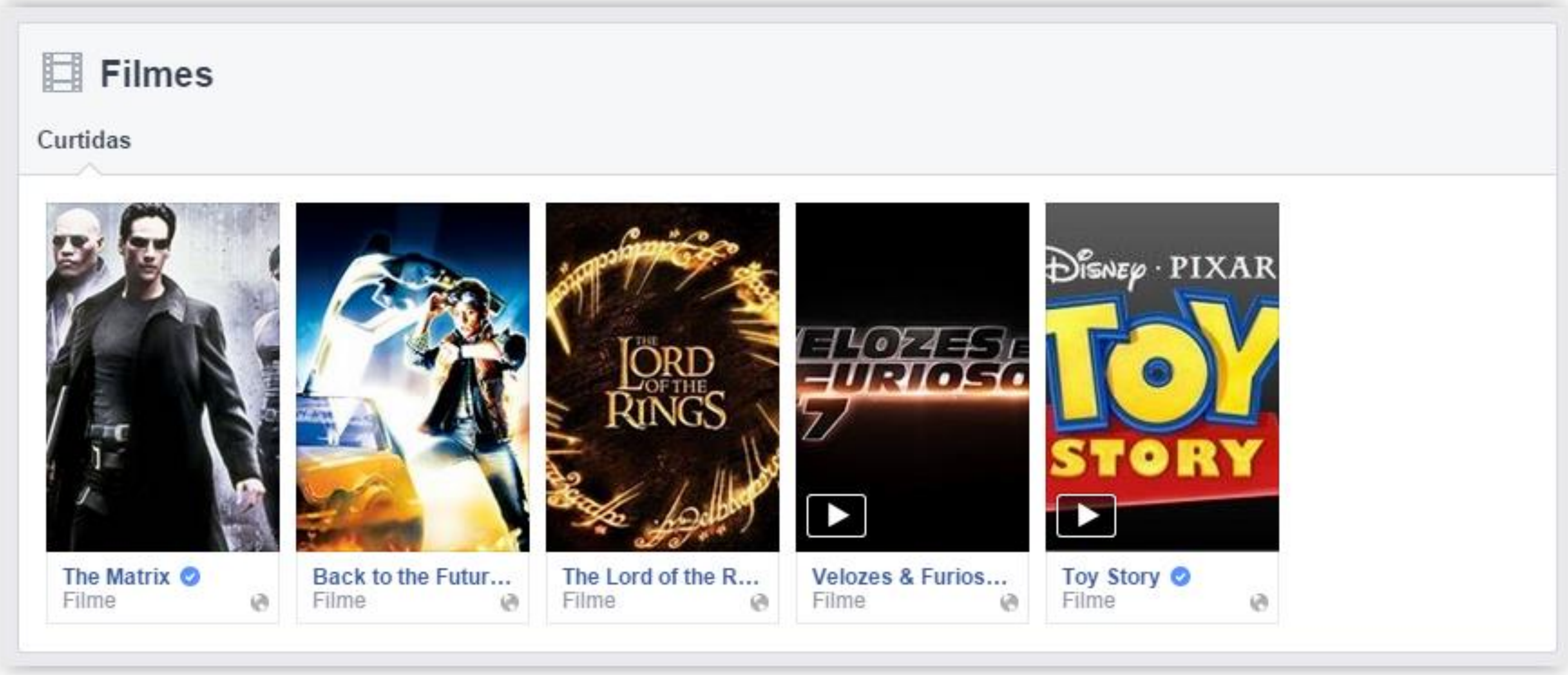
Brute Force: Personal Wlist

Brute Force: Personal Wlist

Brute Force: Personal Wlist



Brute Force: Personal Wlist



Brute Force: Personal Wlist

Teríamos mais sucesso com uma wordlist que contivessem as palavras abaixo:

Tricolor, SPFC, missmine, metálica, (palavras em inglês em geral).

Do que utilizar palavras como:

Timao, Palmeiras, Corinthians, Verdão, Katinguele, Soweto...

Brute Force: Rainbow Tables

O processo de Rainbow Tables é interessante e ajuda muito na velocidade de um ataque de força bruta, mas, possui um problema: Você precisará de muito espaço em disco.

Utilizar rainbow tables é já cifrar as senhas e efetuar a comparação das hashes, sendo assim, você deverá ter um banco de dados com as senhas e seus hashes.

Uma ferramenta muito utilizada para esse tipo de trabalho é o Ophcrack, que tem a função específica de criar hashes e wordlists rainbowtables para ataques à sistemas Operacionais da Micrisoft

Brute Force: Senhas da M$

A Microsoft até a versão do Windows XP e 2003, utilizava o sistema de senhas LM até migrar para o sistema Kerberos, sendo assim, dificultando o trabalho com Rainbow Tables.

Toda e qualquer senha do Windows XP ou 2003 deveriam conter até 14 caracteres, caso a senha do usuário seja inferior, o Windows preenche com o restante dos caracteres nulos até completar 14 no total.

Caso tenha mais do que 14 caracteres, então o Windows descarta os caracteres adicionais, por isso é tão fácil quebrar senhas do Windows utilizando Rainbow Tables.

Você pode constatar isso no site oficial da Microsoft:
https://technet.microsoft.com/pt-br/library/cc716472.aspx

Chega por hoje

www.eSecurity.com.br

E-mail: alan.sanches@esecurity.com.br

Twitter: @esecuritybr e @desafiohacker

Skype: desafiohacker

Fanpage: www.facebook.com/academiahacker